Attorney's Docket No.: 10664-147001

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Gary Liu   Art Unit : 3621
Serial No. : 09/826,320   Examiner : P. Elisca
Filed : April 3, 2001
Title : CERTIFIED TRANSMISSION SYSTEM

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF ON APPEAL

(1) Real Party in Interest

The case is assigned of record to ZixIt Corporation, a Corporation headquartered in Texas, who is the real party in interest.

(2) Related Appeals and Interferences

There are no known related appeals or interferences as indicated in Appendixes B and C.

(3) Status of Claims

Claims 1-19, 22-32 and 36-51 are pending. Claims 1-19, 24-32 and 36-51 stand rejected. Claims 22 and 23 are objected to but would be allowed if amended into independent format. All rejected claims are appealed. Claims 1-41 as pending are provided in Appendix A.

(4) Status of Amendments

No amendments have been filed after non-final Office Action mailed August 17, 2005.

(5) Summary of Claimed Subject Matter

Claims 1, 3-8, 11, 17 and 36 define a computer-implemented method including encrypting a message using a symmetric key (SymmetricKey) to generate an encrypted message (MailContent). Referring to Figs. 1 and 2, the features of the method include the capability of 1)_sending (by a sender A) the encrypted message (e.g., CertifiedMail) to an intended recipient B **without making the symmetric key** (SymmetricKey) **immediately accessible to the intended recipient** B; 2) providing the symmetric key (SymmetricKey) to a third party C; and 3) if the intended recipient B signs and returns to the third party C **a receipt** (e.g., ReceiptSentToRemailer) including a representation of the encrypted message (e.g., CertMailHeader) transferring, by the third party C, **the receipt** (e.g., SignedReceipt) **to a sender** A and **providing the symmetric key** (SymmetricKey) **to the intended recipient** B.
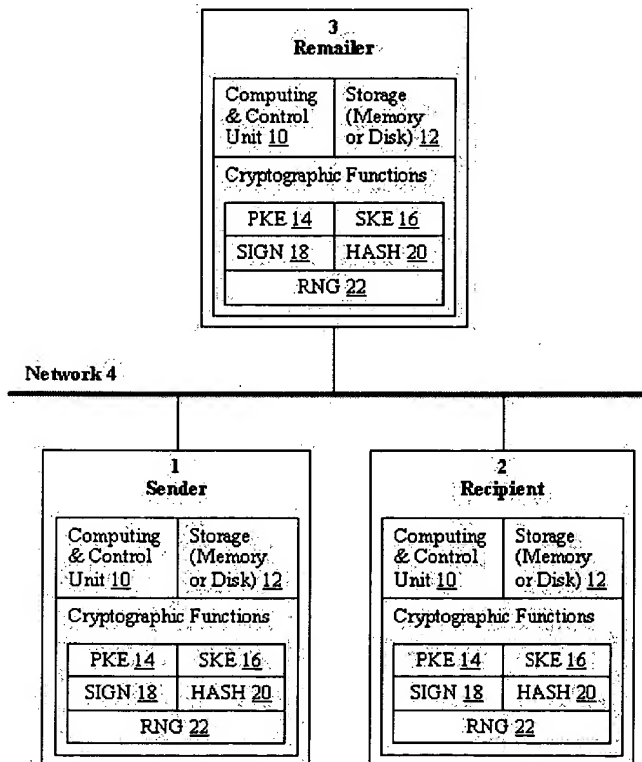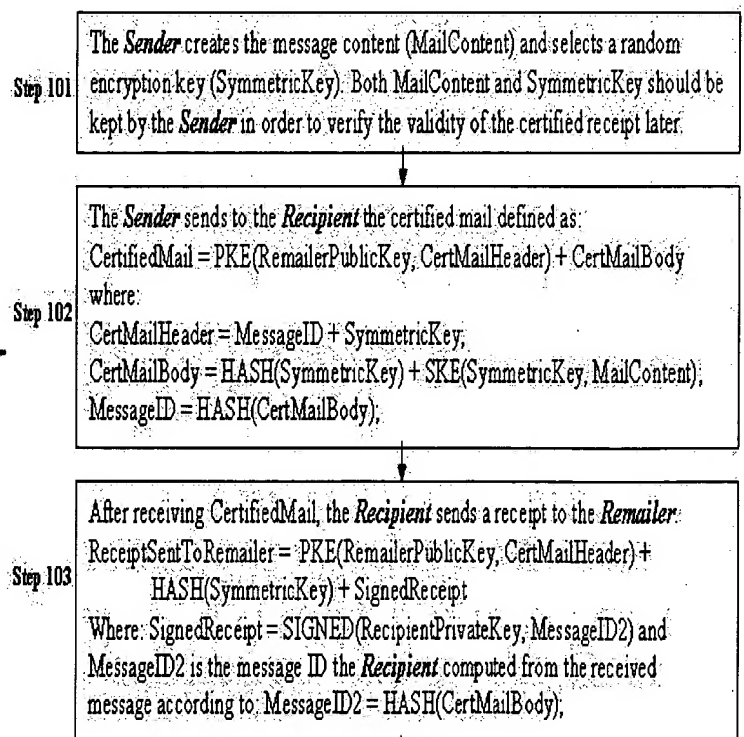

Fig. 1

Fig. 2

Claim 24 defines, in-part, a computer-implemented method for generating a signed receipt certifying that a message has been received at a particular time by an intended recipient, without exposing content of the message. Specifically, the method includes: 1) receiving a message having content encrypted by a symmetric key; 2) receiving a hash of the symmetric key; and 3) **time-stamping a representation** (e.g., via 5 of Fig. 3 and SendTSC) of the hash of the symmetric key and the message encrypted by the symmetric key, including **sending a time stamp certificate** (e.g., Send TSC and Receive TSC) including the representation, a time (e.g., SendTime), and a sender identification (e.g., SenderInfo) and a recipient identification (e.g., ReceipentInfo) for the message (the examples of which are illustrated in Figs. 3 and 4a, and discussed in Applicant's specification at page 17, line 29 to page 22, line 7).

Claim 27 defines, in-part, a computer-implemented method for generating a signed receipt for a message certifying a sending time and a receiving time by an intended recipient without exposing content of the message. The method includes: 1) **receiving a time stamp certificate** including receiving a representation of a hash of a symmetric key and a message encrypted with the symmetric key, a time, and a sender identification and a recipient identification for the message, the time stamp certificate being time-stamped at time of sending (e.g., SendTime); 2) **time-stamping the representation at a time of receiving** (e.g.,ReceiveTime); 3) **combining** the representation time-stamped at the time of sending and the representation time-stamped at the time of receiving **to provide a combined receipt** (e.g., SignedReceipt= SIGNED(RecipientPrivateKey, SendTSC+ReceiveTSC)) (the examples of which are illustrated in Figs. 4b, and discussed in Applicant's specification at page 22, line 8 to page 27, line 21).

Claim 31 defines, in-part, a computer-implemented method for securely sending a message. The method includes: 1) generating a representation of a hash of a symmetric key (e.g., HASH(SymmetricKey) and an encrypted message encrypted using the symmetric key (e.g., SKE(SymmetricKey, MailContent); 2) **sending a request including the representation to a time stamping authority** (e.g., TSC Server); and 3) receiving from the time stamping authority a **time stamp certificate** (e.g., Send TSC and Receive TSC) including a time stamped representation of the hash of the symmetric key and the message encrypted by the symmetric key

(the examples of which are illustrated in Figs. 4b, and discussed in Applicant's specification at page 22, line 8 to page 27, line 21)..

(6)   Grounds of Rejection

Claims 1-21 and 24-51 are rejected under 35 U.S.C § 103(a) as being unpatentable over USP No. 6,549,626 to Al-Salqan in view of US RE No. 38,070E to Spies.

These grounds of rejection are requested to be reviewed on appeal.

(7)   Argument

The rejection of claims 1-21 and 24-51 as allegedly being unpatentable over Al-Salqan in view of Spies is respectfully traversed.

Claim 1 and its dependent Claims

Claim 1 recites in-part encrypting a message using a symmetric key and sending the encrypted message to an intended recipient **without making the symmetric key immediately accessible to the intended recipient**, providing the symmetric key to a third party, and **transferring, by the third party, the receipt to a sender** and **providing the symmetric key to the intended recipient** if the intended recipient signs and returns to the third party a receipt including a representation of the encrypted message.

In the Official Action dated August 17, 2005, the rejection maintains that the foregoing claimed features are disclosed in col. 1 and col. 2 of Al-Salqan (see, pages 2 and 3 of Office Action). However, the cited sections of Al-Salqan do not show the claimed features for at least the following reasons.

I.   Neither Al-Salqan Nor Spies Disclose Sending An Encrypted Message To An Intended Recipient Without Making A Symmetric Key Immediately Accessible To The Intended Recipient

As described above, Applicant respectfully submits that Al-Salqan does not teach sending the encrypted message to an intended recipient **without making a symmetric key** used to encrypt the encrypted message **immediately accessible to the intended recipient**.

Applicant notes that the Examiner reiterates in the Office Action mailed November 4, 2004 and again in the Office Action mailed August 17, 2005 that Al-Salqan discloses the foregoing claimed features in the abstract and at col. 1, lines 29-38 and col. 2, lines 49-64. Applicant respectfully disagrees for the reasons set forth below.

i.   Al-Salqan Does Not Disclose Withholding A Symmetric Key From A Recipient

Al-Salqan at col. 1, lines 29-38 describes a conventional symmetric encryption method used to secure information from misappropriation. Specifically, Al-Salqan discloses using a key to encrypt information and the same key to decrypt the encrypted information. With this method, a message transmitted from the sender to the recipient is symmetrically encrypted as long as the sender and the recipient have **agreed** upon the key.

However Applicant respectfully submits that this is not the same as Applicant's claimed limitation. The Examiner is directed to **M.P.E.P § 2141.02**, under the section entitled "Prior Art Must Be Considered in its Entirety, Including Disclosures that **Teach Away** from the Claims", which sets forth the applicable standard:

> A prior art reference must be considered in its entirety, i.e., as a _whole_, including portions that would **lead away** from the claimed invention. (citing _W.L. Gore & Associates, Inc. v. Garlock, Inc._, 220 USPQ 303 (Fed. Cir. 1983)

In the instant case, the symmetric encryption method disclosed in Al-Salqan's requires that the sender and the recipient first agree upon a symmetric key prior to transmitting an encrypted message. In other words, the symmetric key disclosed in Al-Salqan used for encrypting and decrypting the secured information is already conveyed to the recipient prior to sending the message encrypted by the symmetric key, and the recipient would therefore have the symmetric key at the time of sending. Thus, Al-Salqan expressly teaches away from the claimed invention by having prior agreement between the sender and the recipient so as to determine what this key would be.

As discussed above, Applicant respectfully asserts that this is fundamentally different from Applicant's claimed limitation. Applicant's method includes sending an encrypted message to an intended recipient **without making** a symmetric key used to encrypt the encrypted

message immediately **accessible to the intended recipient**, until, as will be discussed in greater detail later, the recipient has signed and returned a recipient to a third party.

ii. The System Of Al-Salqan Has Access To Private Information Used To Symmetrically Encrypt The Key

Furthermore, Al-Salqan, at col. 2, lines 49-64 and neighboring sections thereof, discloses an asymmetric encryption method that utilizes a public key for encryption and a separate, mathematically related private key for decryption.

More specifically, Al-Salqan discloses encrypting keys for storage, where the key is a private key or key password, such that the key can be decrypted if the key is lost or unavailable (Abstract, lines 1-3). The key to be encrypted, the key to be used to secure the key to be encrypted and private information of the principal are received as input (col. 3, lines 62-67, col. 4, lines 1-2). A principal's private information, such as the principal's mother's maiden name or social security number, is encoded (col. 2, lines 50-52). The encoded result is used to symmetrically encrypt the private key or password (col. 2, lines 52-54). The private key or password is again encrypted using the public key of a trusted party, such as a certification authority (col. 2, lines 54-57). The result of the two encryptions is a key recovery file that may be stored by the principal or other trusted party (col. 2, lines 57-59). When the private key is lost or unavailable, the stored key recovery file can be accessed and decrypted (col. 2, lines 59-63). The principal, or another party available to provide the principal's private information, can retrieve the key recovery file and key (col. 7, lines 21-26).

The Examiner has suggested that this asymmetric method reads on the foregoing claimed features, which Applicant respectfully disagrees, because this asymmetric method does not pertain to **exchanging messages** between a sender and a recipient, and certainly does not include any intended recipient. Indeed, Al-Salqan merely discloses storing a key or key password and allowing the encrypted key or key password to be recovered by the principal or an organization if a private key used to decrypt the encrypted key is lost or otherwise unavailable (col. 2, lines 41-46). That is, Al-Salqan discloses directly storing a key or key password, rather than sending it to a recipient. The key or key password is used by the principal to recover a lost key. This is not the same as Applicant's claimed message exchange process.

II.   Neither Al-Salqan Nor Spies Disclose Transferring, By A Third Party, A Receipt Including A Representation Of An Encrypted Message To A Sender

Claim 1 further recites that if the intended recipient **signs and returns a receipt** including a representation of an encrypted message to the third party, the third party transfers **the receipt** to a sender. Applicant respectfully submits that Al-Salqan does not disclose these claimed features.

Applicant notes that the Examiner reiterates in the Office Action mailed November 4, 2004 and in the Office Action mailed August 17, 2005 that Al-Salqan discloses the foregoing claimed features in the abstract and at col. 1, lines 29-38 and lines 51-67.

As a preliminary matter, the Examiner's grounds of rejection quoted in the Office Action dated August 17, 2005 are substantially the same as those set forth in the Official Action dated November 4, 2004. The Examiner did not respond to the detailed arguments set forth in the previous Amendment filed February 28, 2005 with respect to the foregoing claimed features. Accordingly, without a new rejection or response to the arguments from the Examiner, the deficiencies of the pending rejections as previously argued are still a valid basis for the patentability of claim 1.

Further, even assuming that the Examiner has addressed Applicant's arguments, Applicant's method includes transferring by a third party, the receipt to a sender if the intended recipient signs and returns a receipt including a representation of the encrypted message to the third party. That is, Applicant's particular claim limitation requires two elements: first that a receipt including a representation of an encrypted message be **signed and returned to a third party by the intended recipient**; and second that **the receipt be sent to a sender** by the third party.

The Examiner repeatedly maintained that Al-Salqan discloses the foregoing claimed features, because the trusted party known as a certificate authority issues a certificate which allows third parties to verify the identity of the principal.

However, Applicant respectfully submits that Al-Salqan does not show each of these claimed features for at least the following reasons.

i. The Alleged Intended Recipient Does Not Sign And Return A Receipt Including A Representation Of An Encrypted Message To A Third Party

Al-Salqan fails to disclose that "*the intended recipient signs and returns to the third party a receipt including a representation of the encrypted message.*" The claimed symmetric key is hidden from the intended recipient until a receipt is signed and sent to the third party. The claimed receipt specifically identifies a message corresponding to a symmetric key (e.g., with a message header or hash of the message) and identifies the intended recipient.

In contrast, Al-Salqan discloses using a trusted certification authority to issue a certificate to the third parties in order to verify the identity of the principal. Applicant respectfully submits that this certificate is not the same as Applicant's claimed receipt that is required by the claim limitation. Particularly, certificates are not the same as receipts because certificates do not include a representation of a message associated with a communication between a sender and an intended recipient. Also, the certificate is independent of the message sent between the sender and an intended recipient; that is, the certificate remains the same no matter what message it is attached to.

Furthermore, the certification authority of Al-Salqan merely provides a certificate to ensure identity of a principal. The certificate of Al-Salqan is not signed by the intended recipient nor is it sent to the third party as a condition to receiving the symmetric key as claimed. The certificate does not include the claimed representation of the encrypted message. Thus, Al-Salqan fails to disclose the transferring step.

ii. Al-Salqan Does Not Disclose Transferring, By A Third Party, A Receipt To A Sender

As expressly recited in the pending claims, the claimed receipt, identifying a message and signed by an intended recipient, is provided by the a party to a sender to indicate the receipt of the message by the intended recipient.

However, the certificate of Al-Salqan does not perform such indication, because the certificate does not include a representation of a message associated with a communication between a sender and an intended recipient. Further, Al-Salqan fails to disclose any transmission from the recipient back to the sender, either directly or indirectly. Even assuming that the

certificate of Al-Salqan was returned to the sender from the certificate authority, it is clear that the trusted certification authority does not transfer any receipt to the principal evidencing that the third parties have received any encrypted information.

The Examiner is again directed to **M.P.E.P § 2143.03** under the section entitled "All Claim Limitations Must Be Taught or Suggested", which sets forth the applicable standard:

> To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested *by the prior art*. (citing *In re Royka*, 180 USPQ 580 (CCPA 1974)).

In the instant case, the pending rejection does not "establish *prima facie* obviousness of [the] claimed invention" as recited in the pending claims because the proposed combination fails the "all the claim limitations" standard required under § 103.

II. The Inappropriate Combination of Al-Salqan with Spies

As a preliminary matter, the Examiner has admitted in his official action mailed August 17, 2005 that Al-Salqan does not disclose a receipt that includes a representation of an encrypted message.

The Examiner has suggested that Spies teaches this limitation at col. 5, lines 66-col. 6, line 16, col. 26, lines 1-12 and col. 29, lines 37-49. Applicant respectfully disagrees for at least the following reasons.

i. No Motivation To Combine Al-Salqan and Spies

Applicant would initially stress the requisite motivation to support the ultimate legal conclusion of obviousness under 35 U.S.C. §103 is not an abstract concept but must stem from the applied prior art as a whole and have realistically impelled one having ordinary skill in the art to modify a reference or combine references to arrive at a claimed invention. *In re Newell*, 891 F.2d 899, 13 USPQ2d 1248 (Fed. Cir. 1989). It has been judicially held that a generalization does not establish the requisite motivation to modify a specific reference in a specific manner to arrive at a specifically claimed invention. *In re Deuel*, 51 F.3d 1552, 34 USPQ2d 1210 (Fed. Cir. 1995). Rather, the PTO is required to point out wherein the prior art suggests modifying a

reference or combining references to arrive at a specifically claimed invention. *In re Rouffet*, 149 F.3d 1350, 47 USPQ2d 1543 (Fed. Cir. 1998). In this respect, Applicant would further stress that **the mere identification of claim features in disparate references does not establish the requisite realistic motivation** to support the ultimate legal conclusion of obviousness under 35 U.S.C. §103. *Grain Processing Corp. v. American-Maize Products Co.*, 840 F.2d 902, 5 USPQ2d 1788 (Fed. Cir. 1988).

In the instant case, it is apparent that the Examiner has not established a *prima facie* basis to deny patentability to the claimed invention under 35 U.S.C. §103 for want of the requisite motivation. The Examiner has offered **no explanation why** one having ordinary skill in the art would somehow have been lured to go against the express objectives given by Al-Salqan to modify the system to include sending a receipt representing an encrypted message. *In re Rouffet*; *In re Mayne*.

Indeed, Applicant respectfully submits that the Examiner has provided **no motivation** (let alone a sufficient motivation) to combine Al-Salqan and Spies, and rather has merely provided a citation of Spies that does not support a conclusion of motivation. That one can modify Al-Salqan using the example given in Spies is not in itself a particular motivation to modify the methods taught by Al-Salqan.

Further, that such an action would lead to such obvious efficiencies begs the very question of why Al-Salqan did not teach such a system in the first place. Instead, it appears the Examiner has impermissibly used hindsight in an attempt to reconstruct Applicant's invention. It is improper to use Applicant's disclosure as the motivation to combine the particular teachings in the cited references: "The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in Applicant's disclosure, " **M.P.E.P 2143**, citing *In re Vaeck*, 947 F.2d 488 (Fed. Cir. 1991).

Further, it is respectfully submitted that merely because prior art can be modified is not sufficient to render a claim prima facie obvious (**M.P.E.P. § 2143.01** under the subsection entitled "Fact that References Can Be Combined or Modified is Not Sufficient to Establish Prima Facie Obviousness," which sets forth the applicable standard:

The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. (In re Mills, 16 USPQ2d 1430 (Fed. Cir. 1990))).

In the instant case, even assuming *arguendo* that Al-Salqan can be modified in the manner suggested by the pending Office Action, it is submitted that the "mere fact that [Al-Salqan] can be modified ... does not render the resultant modification obvious" because nowhere does the *prior art* "suggest the desirability of the modification" as set forth by the Office Action. Only Applicant's specification suggests the claimed features of the present invention, whereas the Office Action has attempted to modify Al-Salqan to reach the claimed invention without a motivation and notwithstanding that the prior art does not "suggest the desirability" of the modification.

As discussed above, it is respectfully submitted that the proposed modifications of Al-Salqan are improper because the Examiner has not provided the requisite *objective* evidence *from the prior art* that "suggests the desirability" of the proposed modification. At best, the Examiner has attempted to show only that the elements of the claimed invention (encryption, symmetric key and receipt) are **individually** known without providing a *prima facie* showing of obviousness that the **combination** of elements recited in the claims is known or suggested in the art.

Accordingly, the Examiner's allegations, for example, that the encryption method of Al-Salqan and the purchase receipt of Spies are known separately is irrelevant to the determination of patentability for the *combination* of those features as recited in the pending claims. As is well known in patent law, a *prima facie* showing of obviousness can only be established if the prior art "suggests the desirability" of the proposed combination using *objective* evidence. The Examiner is directed to **M.P.E.P. § 2143.01** under the subsection entitled "Fact that the Claimed Invention is Within the Capabilities of One of Ordinary Skill in the Art is Not Sufficient by Itself to Establish *Prima Facie* Obviousness", which sets forth the applicable standard:

> A statement that modifications of the prior art to meet the claimed invention would have been [obvious] because the references relied upon teach that all aspects of the claimed invention were **individually** known in the art is *not* sufficient to establish a *prima facie* case of obviousness without some objective reason to combine the teachings of the references. (citing *Ex parte Levengood*, 28 USPQ2d 1300 (Bd. Pat. App. & Inter. 1993)).

In the instant case, even assuming *arguendo* that Al-Salqan and the alleged addition of the purchase receipt as disclosed in Spies "teach that all aspects of the claimed invention [are] individually known in the art," it is submitted that such a conclusion "is not sufficient to establish a *prima facie* case of obviousness" because there is no *objective* reason on the record to modify the teachings of the cited prior art. In contrast, the asserted motivations set forth by the Office Action are based solely on hindsight reasoning using only Applicant's specification of what would have been obvious. It is respectfully submitted that only Applicant's specification provides the requisite rationale for the processes recited in the pending claims.

For at least these reasons, it is respectfully submitted that the proposed combination is improper because the prior art does not suggest such a modification to Al-Salqan and there is no objective evidence on the record that suggests the desirability of the proposed combination suggested by the Examiner. It is respectfully submitted that there is no rationale or motivation, derived from the prior art, for modifying Al-Salqan using Spies in the manner set forth by the Examiner.

Claims 2, 30 and 38 depend from claim 1 and are submitted to be allowable at least by virtue of their dependence on claim 1.

Claim 3 and its dependent Claims

Claim 3 is directed to a computer implemented method that includes in-part encrypting a symmetric key to make the symmetric key accessible to a third party **but not immediately accessible** to an intended recipient at a sender, and **signing a receipt including a representation of the encrypted message** at the intended recipient; and **transferring the receipt to the sender** and **providing the symmetric key to the intended recipient** if the receipt is properly signed at the third party.

As discussed above with respect to claim 1, the combination of Al-Salqan and Spies does not disclose any of the foregoing features. Accordingly, claim 3 is allowable at least for analogous reasons set forth above with respect to claim 1.

Claim 39 depends from claim 3 and is submitted to be allowable at least by virtue of their dependence on claim 3.

Claim 4 and its dependent Claims

Claim 4 is directed to a computer implemented method that includes in-part **receiving a signed receipt and an encrypted symmetric key from an intended recipient**, the signed receipt memorializing receipt of the encrypted message by the intended recipient**, transferring the verified receipt to a sender** at a third party, and **providing the symmetric key to the intended recipient** by the third party.

As discussed above with respect to claim 1, the combination of Al-Salqan and Spies does not disclose any of the foregoing features. Accordingly, claim 4 is allowable at least for analogous reasons set forth above with respect to claim 1.

Claims 40-44 depend from claim 4 and are submitted to be allowable at least by virtue of their dependence on claim 4.

Claim 5 and its dependent Claims

Claim 5 is directed to a computer implemented method that includes in-part receiving a separately encrypted message header associated with a message and **a certified receipt originating from an intended recipient**, the certified receipt including **a first message identifier** signed by the intended recipient, decrypting the separately encrypted message header to expose a symmetric key and **a second message identifier**, verifying the certified receipt, including verifying a signature of the intended recipient and that **the first and second message identifiers are the equivalent**, and **forwarding the certified receipt to the sender**.

As discussed above, and as acknowledged by the Examiner, Al-Salqan does not disclose receiving a receipt from the third parties or the trusted certification authority. At best, Al-Salqan discloses only that a certificate is issued to the third parties by the trusted certification authority. However, as is evident, the certificate includes only the identity of the principal, and does not include any message identifier. Even assuming *arguendo* that the Examiner's interpretation has merit, the combination of Al-Salqan and Spies still does not arrive at the claimed invention, because neither Al-Salqan nor Spies disclose or suggest verifying the equivalency of the claimed message identifiers.

In this regard, it is well settled that rejections under 35 U.S.C. §103 must be based upon hard facts. *In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); In re Freed, 425 F.2d*

785, 165 USPQ 570 (CCPA 1970); In re Warner, 379 F.2d 1011, 154 USPQ 173 (CCPA 1967).
Further, in imposing a rejection under 35 U.S.C. §103, the Examiner must point to a **source** in
the applied prior art for each claim limitation as well as a **source** for the requisite motivation.
*Smiths Industries Medical System v. Vital Signs Inc., 183 F.3d 1347, 51 USPQ2d 1415 (Fed. Cir.
1999).* That burden has **not** been discharged.

It is not apparent and the Examiner has failed to point out where in Al-Salqan or Spies
are the claimed first and second message identifiers disclosed, let alone a verification process
that verifies the equivalency of these message identifiers. Having failed to specifically identify
wherein an applied reference discloses each feature of a claimed invention, as claimed, the
Examiner has, in effect, denied Applicant procedural due process of law, in that it is difficult for
Applicant to respond to the rejection by shooting arrows into the dark. *In re Mullin, 481 F.2d
1333, 179 USPQ 97 (CCPA 1973).*

Accordingly, for at least these reasons and those discussed with respect to claim 1, it is
respectfully submitted that claim 5 is allowable.

Claims 45-46 depend from claim 5 and are submitted to be allowable at least by virtue of
their dependence on claim 5.

Claim 6 and its dependent Claims

Claim 6 is directed to a computer implemented method that includes in-part encrypting a
message using a symmetric key, sending the encrypted message to an intended recipient **without
the symmetric key**, forwarding the encrypted symmetric key to a third party, and receiving from
the third party **a certified receip**t verified by the third party indicating receipt of the message by
the intended recipient.

As discussed above, the combination of Al-Salqan and Spies does not disclose or suggest
a certified receipt indicating a receipt of a message received by an alleged recipient.
Furthermore, Al-Salqan discloses only that the sender and the recipient agree upon the
symmetric key prior to message transmission, and therefore does not disclose any need for
forwarding an encrypted symmetric key to a third party. Spies does not cure these deficiencies
of Al-Salqan because the purchaser 302 does not forward the purchaser's symmetric key to any
party, as is evident by the fact that the purchaser does not communicate with any third party

other than the merchant 314. The encrypted PI is decrypted, for example, by the acquirer 306 using its own private key exchange key (see, col. 25, lines 50-51). Similarly, the encrypted GSO is decrypted by the merchant using its own cryptography system and its own key exchange private key (see, col. 25, lines 35-37).

Accordingly, for at least these reasons and those discussed with respect to claim 1, it is respectfully submitted that claim 6 is allowable.

Claims 10 and 47 depend from claim 6 and are submitted to be allowable at least by virtue of their dependence on claim 6.

Claim 7 and its dependent Claims

Claim 7 is directed to a computer implemented method that includes in-part creating a message header that includes a symmetric key and **a message identifier** associated with a message for transmission to an intended recipient, receiving **a certified receipt originating from the intended recipient**, where the certified receipt is **forwarded to a sender** after verification.

As discussed above with respect to claims 1 and 5, the combination of Al-Salqan and Spies does not disclose a message identifier or a certified receipt. Accordingly, claim 7 is allowable at least for analogous reasons set forth above with respect to claims 1 and 5.

Claim 48 depends from claim 7 and is submitted to be allowable at least by virtue of their dependence on claim 7.

Claim 8 and its dependent Claims

Claim 8 is directed to a computer implemented method that includes in-part, at an recipient, creating **a signed receipt** for the encrypted message including signing a hash of the encrypted message and **returning the signed receipt to a third party**, and after verification of the signed receipt at the third party, **receiving the symmetric key** from the third party;.

As is clear from the discussed provided above, the merchant server 304 of Spies generates and digitally signs a purchase receipt 342, and sends the signed receipt to the purchaser 302. However, Spies is completely silent with respect to forwarding the signed receipt to a third

party other than the purchaser 302, let alone disclose verifying the signed receipt by the third party and in response, receiving a symmetric key.

Accordingly, for at least these reasons and those discussed with respect to claim 1, it is respectfully submitted that claim 8 is allowable.

Claims 9 and 49 depend from claim 8 and are submitted to be allowable at least by virtue of their dependence on claim 8.

Claim 11 and its dependent Claims

Claim 11 is directed to a computer implemented method that includes in-part generating a receipt including **generating a message identifier** prior to decrypting a message, the message identifier including a representation of the hash of the symmetric key and the message encrypted by the symmetric key, where the message identifier is able to be used to verify receipt of the message at the intended recipient without exposing the message content to an intended recipient.

As discussed above with respect to claims 1 and 5, the combination of Al-Salqan and Spies does not disclose any message identifier. Specifically, the certificate as disclosed in Al-Salqan is not the same as a receipt because the certificate does not include a representation of a message identifier associated with a communication between a sender and an intended recipient. Also, the certificate is independent of the message sent between the sender and an intended recipient; that is, the certificate remains the same no matter what message it is attached to. Accordingly, claim 11 is allowable at least for analogous reasons set forth above with respect to claims 1 and 5.

Claims 12-16 depend from claim 11 and are submitted to be allowable at least by virtue of their dependence on claim 11.

Claim 17 and its dependent Claims

Claim 17 is directed to a computer implemented method that includes in-part generating a representation of the hash of a symmetric key and a message encrypted by the symmetric key, and signing the representation to **generate a signed receipt**, where the signed receipt is generated **prior** to decrypting the message and receiving the symmetric key.

However, it is respectfully reiterated that the purchaser receipt 342 is generated **after** the order containing the goods and services order (GSO) and the purchaser instruction (PI) placed by the purchaser 302 is processed and decrypted, for example, by the acquirer 306 (GSO) and the merchant server 314 (PI).

Accordingly, for at least these reasons and those discussed with respect to claim 1, it is respectfully submitted that claim 17 is allowable.

Claims 18-19 and 50 depend from claim 17 and are submitted to be allowable at least by virtue of their dependence on claim 17.

Claim 24 and its dependent Claims

Claim 24 is directed to a computer implemented method for generating a signed receipt certifying that a message has been received at a particular time by an intended receipt without exposing content of the message, the method includes in-part generating a representation of the hash of the symmetric key and the message encrypted by the symmetric key, wherein the representation is generated prior to decrypting the message and receiving the symmetric key, and **time-stamping the representation**, including **sending a time stamp certificate** including the representation, a time, and a sender identification and a recipient identification for the message.

However, as discussed in the previous Amendment filed February 28, 2005, Al-Salqan is completely silent with respect to time stamping any certificate or receipt such that it is impossible to generate a signed receipt certifying that the encrypted message has been received at a particular time by an intended recipient, as recited in claim 24. Spies does not cure this deficiency of Al-Salqan, because Spies also does not disclose or suggest any time-related issues, let alone disclose a time stamp certificate, a time or a sender ID or recipient ID for the encrypted message.

Accordingly, for at least these reasons and those discussed with respect to claim 1, it is respectfully submitted that claim 24 is allowable.

Claims 25-26 depend from claim 24 and are submitted to be allowable at least by virtue of their dependence on claim 24.

Claim 27 and its dependent Claims

Claim 27 is directed to a computer implemented method that includes in-part receiving a **time stamp certificate** including a representation of the hash of the symmetric key and the encrypted message, a time, and a sender identification and a recipient identification for the message where the time stamp certificate is time-stamped **at time of sending, time-stamping the representation at a time of receiving**, and **combining the representation** time-stamped at the time of sending and the representation at the time of receiving to provide a combined receipt;

For analogous reasons discussed with respect to claim 24, it is respectfully submitted that neither Al-Salqan nor Spies disclose or suggest a time-stamp certificate or time stamping the time stamp certificate including a representation of the hash of a symmetric key and a message encrypted by the symmetric key at the time of receiving the time stamp certificate.

Furthermore, the combination of Al-Salqan and Spies fails to disclose or suggest time stamping a time stamp certificate at the time of sending and at the time of receiving, let alone disclose providing a combined receipt as a function of the time stamp certificate time-stamped at the time of sending and at the time of receiving.

Accordingly, for at least these reasons and those discussed with respect to claims 1 and 24, it is respectfully submitted that claim 27 is allowable.

Claims 28-29 depend from claim 27 and are submitted to be allowable at least by virtue of their dependence on claim 27.

Claim 31 and its dependent Claims

Claim 31 is directed to a computer implemented method that includes in-part receiving from a **time stamping authority a time stamp certificate** including a time stamped representation of the hash of the symmetric key and the message encrypted by the symmetric key.

However, as discussed above with respect to claims 24 and 27, the combination of Al-Salqan and Spies does not disclose any time stamp certificate. The Examiner also has not identified which element of Al-Salqan and Spies is considered as the claimed time stamp authority.

Accordingly, for at least these reasons and those discussed with respect to claims 24 and 27, it is respectfully submitted that claim 31 is allowable.

Claims 32 and 51 depend from claim 31 and are submitted to be allowable at least by virtue of their dependence on claim 31.

Claim 36 and its dependent Claims

Claim 31 is directed to a computer implemented method that includes in-part sending the encrypted message to an intended recipient **without making the symmetric key immediately accessible** to the intended recipient at a sender, **creating a signed receipt** for the encrypted message, including signing a hash of the encrypted message and **returning the signed receipt to the third party** at the intended recipient, and providing the **symmetric key to the intended recipient** at the third party
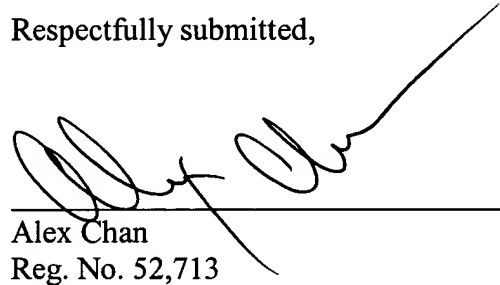
Claim 36 is therefore allowable at least for analogous reasons set forth above with respect to claim 3..

Claim 37 depends from claim 36 and is submitted to be allowable at least by virtue of their dependence on claim 37.

For at least the above reasons, claims 1-19, 24-32 and 36-51 are in condition for allowance, and reversal of the Examiner's rejection to the contrary is respectfully requested.

Please apply $250 for the brief fee and any other charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: March 10, 2006

Alex Chan
Reg. No. 52,713

Fish & Richardson P.C.
500 Arguello Street, Suite 500
Redwood City, California 94063
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

Appendix of Claims

1.   A computer-implemented method, comprising:

encrypting a message using a symmetric key to generate an encrypted message;

sending the encrypted message to an intended recipient without making the symmetric key immediately accessible to the intended recipient;

providing the symmetric key to a third party; and

if the intended recipient signs and returns to the third party a receipt including a representation of the encrypted message, transferring, by the third party, the receipt to a sender and providing the symmetric key to the intended recipient.

2.   The computer-implemented method of claim 1 wherein the receipt signed by the intended recipient contains an identifier computed from the message and the symmetric key using a cryptographically secure hash function.

3.   A computer-implemented method, comprising:

at a sender, encrypting a message using a symmetric key, encrypting the symmetric key to make the symmetric key accessible to a third party but not immediately accessible to an intended recipient and sending the encrypted message and the encrypted symmetric key to the intended recipient;

at the intended recipient, signing a receipt including a representation of the encrypted message and sending the receipt and the encrypted symmetric key to the third party; and

at the third party, transferring the receipt to the sender and providing the symmetric key to the intended recipient if the receipt is properly signed.

4.   A computer-implemented method for certifying receipt of a message, the message being sent from a sender to an intended recipient and being encrypted by a symmetric key, and the method executing at a third party distinct from the sender and the intended recipient, the method comprising:

receiving a signed receipt and an encrypted symmetric key from an intended recipient, the signed receipt memorializing receipt of the encrypted message by the intended recipient;

verifying the signed receipt;

transferring the verified receipt to a sender; and

providing the symmetric key to the intended recipient.

5.   A computer-implemented method for certifying receipt of a message, the message being sent from a sender to an intended recipient and being encrypted by a symmetric key, the method executing at a third party distinct from the sender and the intended recipient, the method comprising:

receiving a separately encrypted message header associated with a message and a certified receipt originating from an intended recipient, the certified receipt including a first message identifier signed by the intended recipient;

decrypting the separately encrypted message header to expose a symmetric key and a second message identifier;

verifying the certified receipt, including verifying a signature of the intended recipient and that the first and second message identifiers are the equivalent; and

after verifying the certified receipt, forwarding the certified receipt to the sender; and forwarding the symmetric key to the intended recipient.

6.   A computer-implemented method, comprising:

encrypting a message using a symmetric key;

sending the encrypted message to an intended recipient without the symmetric key;

forwarding the encrypted symmetric key to a third party; and

receiving from the third party a certified receipt verified by the third party indicating receipt of the message by the intended recipient.

7.   A computer-implemented method, comprising:

creating a message header that includes a symmetric key and a message identifier associated with a message for transmission to an intended recipient;

encrypting the message using the symmetric key;

public key encrypting the message header using a public key of a third party;

attaching the message header to the encrypted message forming a certified message and forwarding the certified message to the intended recipient;

receiving a certified receipt originating from the intended recipient, the certified receipt being verified at the third party and forwarded to a sender after verification; and

verifying validity of the receipt using the stored symmetric key and the certified message.

8.   A computer-implemented method for providing a receipt for a message, the message being sent from a sender to an intended recipient and the method executing at the recipient, the method comprising:

receiving an encrypted message from a sender, the encrypted message encrypted by a symmetric key;

creating a signed receipt for the encrypted message including signing a hash of the encrypted message and returning the signed receipt to a third party;

after verification of the signed receipt at the third party, receiving the symmetric key from the third party; and

decrypting the encrypted message using the symmetric key.

9.   The computer-implemented method of claim 8 wherein the step of receiving the symmetric key includes not receiving the symmetric key until a successful transfer of the signed receipt to the sender.

10.   The computer-implemented method of claim 6, further comprising:

storing a copy of the certified receipt and the symmetric key; and

verifying the validity of the certified receipt using the stored symmetric key and the certified message.

11.   A computer-implemented method for generating a receipt associated with a message, where the receipt is created without exposing content of the message to an intended recipient, comprising:

receiving a message encrypted by a symmetric key;

receiving a hash of the symmetric key; and

generating a receipt including generating a message identifier prior to decrypting the message, the message identifier including a representation of the hash of the symmetric key and

the message encrypted by the symmetric key,

wherein the message identifier is able to be used to verify receipt of the message at the intended recipient without exposing the message content to an intended recipient.

12. The computer-implemented method of claim 11, wherein:

generating a receipt including includes using a hash function to generate the message identifier.

13. The computer-implemented method of claim 11, further comprising:

receiving a first message identifier at the intended recipient;

the generating step including generating a receipt including a second message identifier, at the intended recipient; and

sending the receipt and the first message identifier to a third party.

14. The computer-implemented method of claim 13, further comprising:

receiving the receipt, at the third party;

verifying the receipt without accessing message content; and

providing the receipt to a sender.

15. The computer-implemented method of claim 11, where:

the message is encrypted with the symmetric key prior to sending to the intended recipient; and

the symmetric key is sent to the intended recipient from a third party so that the intended recipient can decrypt the message.

16. The computer-implemented method of claim 11, further comprising:

sending the encrypted symmetric key to the intended recipient with the message;

at the intended recipient, sending the encrypted symmetric key to a third party with a receipt that includes a representation of the message identifier; and

sending the receipt to a sender after verification of the receipt.

17.   A computer-implemented method for generating a signed receipt associated with a message without exposing content of the message, comprising:

receiving a message encrypted by a symmetric key;

receiving a hash of the symmetric key;

generating a representation of the hash of the symmetric key and the message encrypted by the symmetric key; and

signing the representation to generate a signed receipt,

wherein the signed receipt is generated prior to decrypting the message and receiving the symmetric key.

18.   The computer-implemented method of claim 17, further comprising:

sending the signed receipt to a third party for transfer to a sender; and

verifying validity of the signed receipt at the third party.

19.   The computer-implemented method of claim 18, further comprising:

allowing a recipient access to content of the message if the signed receipt is verified at the third party.

20-21. (Canceled)

22.   A computer-implemented method for time-stamping a message without exposing content of the message to a time stamping authority, comprising:

encrypting a message using a symmetric key;

computing a hash of the symmetric key;

generating a representation of the hash of the symmetric key and the message encrypted by the symmetric key; and

time-stamping the representation, including sending the representation to a time-stamping authority and receiving from the time-stamping authority a time stamp certificate including the representation, a time, and a sender identification and a recipient identification for the message.

23.   A computer-implemented method for time-stamping a message without exposing content of the message to a time stamping authority, comprising:

encrypting a message using a symmetric key;

computing a hash of the symmetric key;

generating a representation of the hash of the symmetric key and the message encrypted by the symmetric key; and

time-stamping the representation, including sending the representation to a time-stamping authority and receiving from the time-stamping authority a time stamp certificate including the representation, a time, a sender identification and a recipient identification for the message and at least one of a public key of the sender and a public key of the recipient.

24. A computer-implemented method for generating a signed receipt certifying that a message has been received at a particular time by an intended recipient, without exposing content of the message, comprising:

receiving a message having content, wherein the message is encrypted by a symmetric key;

receiving a hash of the symmetric key;

generating a representation of the hash of the symmetric key and the message encrypted by the symmetric key, wherein the representation is generated prior to decrypting the message and receiving the symmetric key; and

time-stamping the representation, including sending a time stamp certificate including the representation, a time, and a sender identification and a recipient identification for the message.

25. The computer-implemented method of claim 24, further comprising:

sending the time-stamped representation to a third party such that the time stamp can be verified by the third party without exposing the content of the message to the third party; and

verifying validity of the signed receipt at the third party.

26. The computer-implemented method of claim 25, further comprising:

allowing an intended recipient access to the content of the message if the signed receipt is verified at the third party.

27.   A computer-implemented method for generating a signed receipt for a message certifying a sending time and a receiving time by an intended recipient without exposing content of the message, comprising:

receiving a message encrypted with a symmetric key;

receiving a hash of the symmetric key;

receiving a time stamp certificate including a representation of the hash of the symmetric key and the encrypted message, a time, and a sender identification and a recipient identification for the message, the time stamp certificate being time-stamped at time of sending;

time-stamping the representation at a time of receiving;

combining the representation time-stamped at the time of sending and the representation time-stamped at the time of receiving to provide a combined receipt;

signing the combined receipt; and

sending the combined receipt to a third party such that the combined receipt can be verified by the third party without exposing content of the message to the third party.

28.   The computer-implemented method of claim 27, further comprising:

verifying validity of the signed receipt at the third party.

29.   The computer-implemented method of claim 27, further comprising:

allowing an intended recipient access to the content of the message if the signed receipt is verified at the third party.

30.   The computer-implemented method of claim 1, further comprising:

computing a hash of the symmetric key; and

making the hash of the symmetric key accessible to the intended recipient, wherein the receipt contains a representation of the symmetric key.

31.   A computer-implemented method for securely sending a message, comprising:

encrypting a message using a symmetric key;

computing a hash of the symmetric key; and

generating a representation of the hash of the symmetric key and the encrypted message;

sending a request including the representation to a time stamping authority;

receiving from the time stamping authority a time stamp certificate including a time stamped representation of the hash of the symmetric key and the message encrypted by the symmetric key;

generating a certified message including the time stamp certificate; and

sending the certified message to a recipient.

32.   The computer-implemented method of claim 31, wherein:
generating the representation includes using a one-way hash.

33.-35. (Canceled)

36.   A computer-implemented method of for securely sending and receiving a message, using a third party to verify authenticity of the message, comprising:
at a sender:
        encrypting a message using a symmetric key to generate an encrypted message;
        sending the encrypted message to an intended recipient without making the symmetric key immediately accessible to the intended recipient; and
        providing the symmetric key to a third party;
at the intended recipient:
        receiving the encrypted message from the sender;
        creating a signed receipt for the encrypted message, including signing a hash of the encrypted message and returning the signed receipt to the third party;
        after verification of the signed receipt at the third party, receiving the symmetric key from the third party; and
        decrypting the encrypted message using the symmetric key;
at the third party:
        receiving the signed receipt from the recipient;
        verifying the signed receipt;
        transferring the verified receipt to the sender; and
        providing the symmetric key to the intended recipient.

37.   The computer implemented method of claim 36, wherein:

at the sender:

sending the encrypted message to the intended recipient includes encrypting the symmetric key with a public key of the third party and sending the encrypted symmetric key to the intended recipient so that the intended recipient cannot access the symmetric key or the message prior to the intended recipient returning the signed receipt to the third party; and

encrypting the message using a symmetric key to generate the encrypted message includes creating a first hash of encrypted content of the message and including the first hash of the encrypted content in the encrypted message;

at the intended recipient:

returning the signed receipt to the third party includes creating a second hash of the encrypted content in the message, sending the second hash of the encrypted content in the message, forwarding the encrypted symmetric key to the third party for the third party to decrypt the key, but not sending the encrypted message to the third party;

at the third party:

providing the symmetric key to the intended recipient after verifying the signed receipt from the intended recipient;

verifying the signed receipt includes verifying that the first hash of the encrypted content equals the second hash of the encrypted content; and

providing the symmetric key to the intended recipient includes decrypting the encrypted symmetric key sent by the recipient.

38.   The computer-implemented method of claim 1, wherein:

sending the encrypted message to the intended recipient includes encrypting the symmetric key with a public key of the third party and sending the encrypted symmetric key to the intended recipient so that the recipient cannot access the symmetric key or the message prior to the intended recipient returning the signed receipt to the third party; and

encrypting a message using a symmetric key to generate an encrypted message includes creating a first hash of encrypted content of the message and including the first hash of the encrypted content in the encrypted message.

39.   The computer-implemented method of claim 3, further comprising:

at the sender, creating a first hash of encrypted content of the message and sending the first hash to the recipient;

at the recipient, creating a second hash of the encrypted content in the message, sending the second hash to the third party and decrypting the encrypted message after receiving the symmetric key from the third party; and

at the third party, comparing the first hash to the second hash to verify that the first hash is equal to the second hash, decrypting the encrypted symmetric key, wherein providing the symmetric key does not occur until after comparing the first and second hashes.

40.   The computer-implemented method of claim 4, further comprising:

decrypting the encrypted symmetric key for providing to the intended recipient.

41.   The computer-implemented method of claim 40, wherein:

decrypting the encrypted symmetric key includes decrypting the encrypted symmetric key received from the intended recipient, wherein the intended recipient received the encrypted symmetric key from the sender.

42.   The computer-implemented method of claim 4, wherein:

providing the symmetric key to the intended recipient occurs after verifying the signed receipt.

43.   The computer-implemented method of claim 4, wherein:

verifying the signed receipt includes determining that a hash of the encrypted message created by the sender is equivalent to a hash of the encrypted message created by the intended recipient.

44.   The computer-implemented method of claim 4, wherein:

verifying the signed receipt ensures that the intended recipient received an encrypted message sent by the sender.

45.   The computer-implemented method of claim 5, wherein the message identifier includes a hash of the encrypted message, the method further comprising: verifying that the message identifier signed by the intended recipient equals the message identifier in the separately encrypted message header.

46.   The computer-implemented method of claim 5, wherein: forwarding the symmetric key to the intended recipient occurs after verifying the certified receipt.

47.   The computer-implemented method of claim 6, wherein: forwarding the encrypted symmetric key to the third party without exposing the message to the third party.

48.   The computer-implemented method of claim 7, wherein the method does not include sending the message to the third party.

49.   The computer-implemented method of claim 8, further comprising:

receiving a first hash of the encrypted message from the sender;

hashing the encrypted message to create a second hash of the encrypted message; and

sending the first and second hashes to the third party for the third party to verify that the first hash equals the second hash.

50.   The computer-implemented method of claim 17, further comprising:

receiving a first hash of encrypted content;

hashing the received encrypted message content to create a second hash of the encrypted content; and

sending the first and second hashes to a third party for verification.

51.   The computer-implemented method of claim 31, further comprising:

sending the representation of the hash of the symmetric key and the encrypted message to an intended recipient, wherein the intended recipient does not have access to the symmetric key for decrypting the encrypted message at the time of receipt.

Appendix B of Evidence

None.

Appendix C of Related Proceedings

None.

50324759.doc